UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

WILLIAMSON GRANADOS, individually and on behalf of all others similarly situated, Plaintiff, v. MR. COOPER GROUP, INC., Defendant.	Civil Action No. 3:23-cv-02522 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Williamson Granados (hereinafter, "Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to himself and on information and belief as to all other matters, by and through his counsel, hereby brings this Class Action Complaint against Defendant Mr. Cooper Group, Inc. (hereinafter, "Mr. Cooper" or "Defendant").

I. INTRODUCTION

1. On or around October 31, 2023, Mr. Cooper lost control over its customers' highly sensitive personal information in a data breach perpetrated by cybercriminals (the "Data Breach").

2. The Data Breach exposed the personal information belonging to what is estimated to be 4.3 million customers, and, upon information and belief, includes names, Social Security numbers, addresses, phone numbers, dates of birth, zip code, and states of residence—information used by Mr. Cooper for its business operations (hereinafter, the "Personal Information"). That

exposure disturbs customers, as they no longer control their highly sensitive and confidential Personal Information, cannot stop others from viewing it, cannot prevent criminals from misusing it, and crucially cannot control where and to whom that Personal Information is sold and subsequently used.

3. Plaintiff received Mr. Cooper's Data Breach notice on November 2, 2023.

4. Plaintiff brings this Class Action on behalf of himself and all others harmed by Mr. Cooper's misconduct.

II. PARTIES

5. Plaintiff is an individual California citizen residing in Los Angeles County, California.

6. Defendant Mr. Cooper is a corporation organized under the state laws of Delaware with its principal place of business located at 8950 Cypress Waters Blvd., Coppell, Texas 75019, Dallas County, Texas. The registered agent for service of process is Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701-3218.

III. JURISDICTION & VENUE

7. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant.

8. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

9. Defendant is headquartered and has its principal place of business of and/or routinely conducts business in the Dallas Division of the Northern District of Texas, has sufficient minimum contacts in this State, has intentionally availed itself of this jurisdiction by marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within this State.

10. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims took place within the Dallas Division of the Northern District of Texas and Defendant is headquartered and/or does business in the Dallas Division of the Northern District of Texas.

IV. FACTUAL ALLEGATIONS

A. Appropriate Cybersecurity Measures are Crucial for Companies that Collect, Store, and Use Sensitive and Confidential Information.

11. Industry leaders recognize that companies need to improve their defenses, particularly how sensitive and confidential information is stored. Rob Carey, former principal deputy chief information officer for the Department of Defense, acknowledged that in years past companies "would do what was necessary, but maybe not sufficient" to protect consumers' data.[1] With the recent updates from the White House's cybersecurity strategy, Mr. Carey suggests that companies "close[] the gap between necessary and sufficient levels of cyber defense and what is expected" to secure and protect consumers' sensitive and confidential information.[2] Indeed, "the cost of preparation and sort of defense is far less than cleaning up a cyber spill . . . or cyber-attack."[3]

---

[1] Lauren Williams, *Companies Prepare to Spend More on Cybersecurity Under New Rules*, Defense One (March 7, 2023), available at: https://www.defenseone.com/defense-systems/2023/03/companies-prepare-spend-more-cybersecurity/383723 (last visited Nov. 12, 2023).
[2] *Id.*
[3] *Id.*

12. A survey of 683 chief information officers and IT executives revealed that the mean IT budget devoted to cybersecurity was 15%, with nearly one quarter of organizations (23%) devoting 20% or more of their IT budget to security.[4] That same survey resulted in 40% of the respondents admitting that the need to increase cybersecurity protections was paramount to improving customer experience, growing the business, transforming existing business processes, and improving profitability.[5]

13. It is undisputed that cybersecurity is crucial where consumers' sensitive and confidential information is stored by companies and organizations. However, despite the threat environment increasing, in 2023, IT and cybersecurity departments were the second most impacted by layoffs and cost cutting.[6]

14. A survey from 2022 revealed that only 17% of organizations polled had performed an audit of their cybersecurity vulnerabilities within the preceding 12 months, 17% of organizations had cybersecurity training for employees in the last 12 months, and just 34% had business continuity plans that covered cybersecurity.[7]

B. Mr. Cooper Collects and Promises to Protect Customers' Confidential Information.

15. Mr. Cooper is a home loan, mortgage refinancing, and debt collection company. It holds loans worth an impressive $937 billion, making it the largest servicer in the nation.

---

[4] Bob Violino, How much should you spend on security?, CSO Online (Aug. 20, 2019), available at: https://www.csoonline.com/article/567633/how-much-should-you-spend-on-security.html (last visited Nov. 12, 2023).

[5] *Id*.

[6] *Global Survey Reveals Cybersecurity Budgets Should be Spent on Security Operations in 2023*, Arctic Wolf (Jan. 23, 2023), available at https://arcticwolf.com/resources/blog/cybersecurity-budgets-spent-security-operations-2023 (last visited Nov 12, 2023).

[7] Johnty Morgan, *How much should you be spending on your cybersecurity?*, Gallagher (April 6, 2022), available at: https://www.ajg.com/uk/news-and-insights/2022/april/spending-on-your-cybersecurity/ (last visited Nov. 12, 2023).

16. To operate its business, Mr. Cooper must create, collect, and store customers' Personal Information.

17. As a result, Mr. Cooper requires its customers to disclose their Personal Information to receive Mr. Cooper's services, including their names, social security numbers, addresses, phone numbers, and dates of birth.

18. In doing so, Mr. Cooper promises those customers that it will protect their information under state and federal law and its internal policies.

19. However – as evidenced by its loss of control of its customers' data – Mr. Cooper never implemented the security safeguards sufficient to fulfill those duties, failing to adequately train its employees on data security, develop policies to prevent breaches, enforce those policies, follow industry standard guidelines on cybersecurity, and timely respond to data breaches and inform customers as required by law. As a result, Mr. Cooper left customers' Personal Information a vulnerable target for theft and misuse.

20. Certainly, on or around October 31, 2023, Mr. Cooper lost control over its customer's highly sensitive Personal Information in a data breach perpetrated by cybercriminals (the "Data Breach").

21. The Data Breach exposed the Personal Information belonging to what is estimated to be 4.3 million customers, including names, social security numbers, addresses, phone numbers, dates of birth, zip code, and state of residence. That exposure disturbs customers, as they no longer control their highly sensitive and confidential Personal Information, cannot stop others from viewing it, cannot prevent criminals from misusing it, and crucially cannot control where and to whom that Personal Information is sold and subsequently used.

C. Plaintiff's Experience

22. Plaintiff is a current Mr. Cooper customer.

23. Plaintiff received a notice from Mr. Cooper of the Data Breach on November 2, 2023.

24. Plaintiff provided his Personal Information to Mr. Cooper and trusted that Mr. Cooper would use reasonable measures to protect it. Accordingly, Plaintiff expected that his Personal Information would be protected according to state and federal law and any applicable internal policies at Mr. Cooper. Upon information and belief, Plaintiff is a victim of the Data Breach.

25. Since the Data Breach, Plaintiff has experienced a dramatic increase in spam calls related to his financial information.

26. To deal with the problems stemming from the Data Breach, Plaintiff has devoted hours to remediating it and mitigating the potential for it to happen again.

27. Indeed, Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what Personal Information was exposed in the Data Breach.

28. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

29. Plaintiff does not recall ever learning that his information was compromised in a data breach incident, other than the Data Breach at issue in this case.

30. Plaintiff suffers a present injury from the increased risk of fraud, identity theft, and misuse resulting from his Personal Information being placed in the hands of criminals. Plaintiff

has a continuing interest in ensuring that his Personal Information, which is the type that cannot be changed and upon information and belief remains in Mr. Cooper's possession, is protected and safeguarded from future breaches.

D. Mr. Cooper has not implemented changes to its business practices to prevent further data breaches. Plaintiff and the Class Face Significant Risk of Continued Identity Theft.

31. Plaintiff and Class Members have suffered injury from the misuse of their Personal Information that can be directly traced to Mr. Cooper.

32. As a result of Mr. Cooper's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including but not limited to monetary losses, and lost time. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how Plaintiff's Personal Information is used;

b. The compromise and continuing publication of Plaintiff's Personal Information;

c. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

d. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

e. Delay in receipt of tax refund monies;

f. Unauthorized use of stolen Personal Information; and

g. The continued increased risk to Plaintiff or her Personal Information, which remains in the possession of Mr. Cooper and is subject to further breaches so long as Mr. Cooper fails to undertake the appropriate measures to protect the Personal Information in its possession.

33. Stolen Personal Information is one of the most valuable commodities on the criminal information black market. According to Experian (a credit-monitoring service) stolen Personal Information can be worth up to $1,000.00 depending on the type of information obtained. Thus, criminals willingly pay money for access to Personal Information, which enables those criminals to commit fraud and identity theft to the detriment of patients and consumers, including Plaintiff and members of the Class.

34. The value of Plaintiff's and Class Members' Personal Information on the black market is considerable. Stolen Personal Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

35. It can take victims years to spot identity or Personal Information theft, giving criminals plenty of time to use that information for cash.

36. One such example of criminals using Personal Information for profit is the development of "Fullz" packages.

37. Cyber-criminals can cross-reference two sources of Personal Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

38. The development of "Fullz" packages means that stolen Personal Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' names, social security numbers, addresses, phone numbers, dates of birth, and other identifiers. In other words, even if certain types of information may not be included in the Personal Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a "Fullz" package and sell

it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and Class Members' stolen Personal Information are being misused, and that such misuse is fairly traceable to the Data Breach.

39. Mr. Cooper disclosed the Personal Information of Plaintiff and Class Members to unauthorized third parties to use in the conduct of criminal activity. Specifically, Mr. Cooper exposed the Personal Information of the Plaintiff and Class Members to people engaged in disruptive and unlawful business practices and tactics.

40. Mr. Cooper's failure to properly and timely notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their Personal Information and take other necessary steps to mitigate the harm caused by the Data Breach.

41. Had Mr. Cooper timely and properly notified Plaintiff and Class Members of the Data Breach, Plaintiff and Class Members could have taken proactive, rather than reactive, mitigating measures. Had Plaintiff received timely notice, he could have placed a freeze on Plaintiff credit and taken other precautions, which would mitigate exposure to criminal activity.

E. Mr. Cooper failed to adhere to FTC Guidelines.

42. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Mr. Cooper, should employ to protect against the unlawful exposure of Personal Information.

43. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide

for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

44. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

45. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

46. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

47. Mr. Cooper's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' (*i.e.*, consumers') Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

V. CLASS ALLEGATIONS

48. This action is brought, and may be properly maintained, as a class action under Rule 23 of the Federal Rules of Civil Procedure. All requisite elements of Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3) are satisfied; as this is a well-defined community of interests in the litigation, the proposed Class and any subclasses are ascertainable, and a single class action is the superior manner to proceed when compared to the joinder of thousands, or tens of thousands, of individual cases challenging the same practices.

49. Plaintiff brings this action individually on behalf of himself, and on behalf of the Class below, of which Plaintiff is a member, under Rule 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure seeking damages, restitution, injunctive and declaratory relief pursuant to the applicable laws set forth in the state law counts below.

50. This action is brought on behalf of a national class (the "Class"), consisting of:

> All ascertainable persons impacted by the Data Breach, including all who Defendant sent a notice of the Data Breach.

51. The Class Period for the Class dates back to the longest applicable statute of limitations for any claims asserted on behalf of that Class from the date this action was commenced and continues through the present and to the date of judgment.

52. Excluded from the Class are Defendant, its corporate parent, subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, and the legal representatives, assigns of any such excluded persons or entities, and the attorneys for Plaintiff herein. Also excluded from the Class are any judges presiding over these proceedings and their immediate family members.

53. **Numerosity**: The members of the Class are so numerous that joinder of all members is impracticable. While the exact numbers of Class members are unknown to Plaintiff at

this time, Plaintiff on information and belief believes that the numbers exceed 100.

54. **Common Questions of Law and Fact Predominate**: The questions of law and fact common to the Class predominate over questions affecting only individuals. Among the questions of law and fact common to the Class are:

a. Whether Mr. Cooper violated state and federal laws by failing to properly store, secure, and dispose of Plaintiff's and Class Members' Personal Information;

b. Whether Mr. Cooper failed to employ reasonable and adequate data and cybersecurity measures in compliance with applicable state and federal regulations;

c. Whether Mr. Cooper acted willfully, recklessly, or negligently regarding securing Plaintiff's and Class Members' Personal Information;

d. How the Data Breach occurred;

e. Whether Mr. Cooper owed a duty to Class Members to safeguard their Personal Information;

f. Whether Mr. Cooper breached their duty to Class Members to safeguard their Personal Information;

g. Whether computer hackers obtained Class Members' Personal Information in the Data Breach;

h. Whether Mr. Cooper knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Mr. Cooper's acts breaching an implied contract they formed with Plaintiff and the Class Members;

j. Whether Mr. Cooper violated the Federal Trade Commission Act

k. Whether Mr. Cooper's conduct was negligent;

l. Whether Mr. Cooper's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Mr. Cooper failed to timely notify Plaintiff and Class Members of the Data Breach;

n. Whether Mr. Cooper was unjustly enriched to the detriment of Plaintiff and the Class;

o. Whether Plaintiff and Class Members are entitled to restitution, damages, compensation, or other monetary relief; and

p. Whether Plaintiff and Class Members are entitled to injunctive and declaratory relief necessary to secure their Personal Information from further intrusion, exposure, and misuse.

55. Common sources of evidence may also be used to demonstrate Mr. Cooper's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Mr. Cooper's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach. Mr. Cooper has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Mr. Cooper's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these

common issues in a single action has important and desirable advantages of judicial economy.

56. **Typicality**: Plaintiff's claims are typical of other Class members' claims because Plaintiff, like every other Class member, was exposed to virtually identical conduct and was compromised in the Data Breach.

57. **Adequacy**: Plaintiff can fairly and adequately represent the Class's interests; Plaintiff has no conflicts of interest with other Class members and has retained counsel competent and experienced in data breach litigation, class actions and complex civil litigation.

58. **Ascertainability**: The identities of individual Class members are readily ascertainable through appropriate discovery from business records maintained by Mr. Cooper and their agents.

59. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy because joinder of all members is impracticable, the likelihood of individual Class members prosecuting separate claims is remote and individual members do not have a significant interest in individually controlling the prosecution of separate actions. No difficulty will be encountered in this case's management to preclude maintenance as a class action.

60. **Manageability**: The Class litigation will be manageable because all issues are identical, and individualized calculation of damages can be accomplished methodically by an expert via the use of data and information provided by Mr. Cooper and its agents.

61. Plaintiff and Class Members have suffered injury, harm, and damages because of Mr. Cooper's unlawful and wrongful conduct. Absent a class action, Mr. Cooper will continue to inadequately maintain Plaintiff's and Class Members' Personal Information that could be subject to future breaches due to lax or non-existent cybersecurity measures, and such unlawful and

improper conduct should not go unchecked nor remedied. Absent a class action, the Class Members will not be able to effectively litigate these claims and will suffer further harm and losses, as Mr. Cooper will be allowed to continue such conduct with impunity and benefit from its unlawful conduct.

VI. CLAIMS FOR RELIEF

COUNT I
Negligence
On Behalf of Plaintiff and the Class

62. Plaintiff realleges the foregoing paragraphs as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

63. Mr. Cooper had a duty to exercise reasonable care and protect and secure Plaintiff's and Class Members' Personal Information. This duty exists at common law and is also codified under Federal law (*see*, *e.g.*, FTCA).

64. Through its acts and omissions, Mr. Cooper breached its duty to use reasonable care to protect and secure Plaintiff's and Class Members' Personal Information by employing substandard or non-existent data and cybersecurity protocols.

65. Mr. Cooper further breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

66. It was reasonably foreseeable, particularly given legal mandates governing financial data protection and the growing number of data breaches of Personal Information— including past data breaches at Mr. Cooper—that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal Information would result in an unauthorized third-party again gaining access

to Mr. Cooper's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Personal Information.

67. Plaintiff's and Class Members' Personal Information constitutes personal property that was stolen due to Mr. Cooper's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

68. Mr. Cooper's negligence directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Personal Information and Plaintiff and Class Members have suffered and will continue to suffer damages because of Mr. Cooper's conduct. Plaintiff and Class Members seek damages and other relief because of Mr. Cooper's negligence.

COUNT II
Negligence Per Se
On Behalf of Plaintiff and the Class

69. Plaintiff realleges the foregoing paragraphs as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

70. Mr. Cooper's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Mr. Cooper, of failing to employ reasonable measures to protect and secure Personal Information.

71. Mr. Cooper violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Personal Information and not complying with applicable industry standards. Mr. Cooper's conduct was particularly unreasonable given the nature and amount of Personal Information it obtains and stores, and the foreseeable consequences of a data breach involving Personal Information including, specifically, the substantial damages

that would result to Plaintiffs and the other Class Members.

72. Mr. Cooper's violations of Section 5 of the FTCA constitutes negligence per se.

73. Plaintiffs and Class Members are within the class of persons that Section 5 of the FTCA were intended to protect.

74. The harm occurring because of the Data Breach is the type of harm Section 5 of the FTCA were intended to guard against.

75. It was reasonably foreseeable to Mr. Cooper that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' Personal Information to unauthorized individuals.

76. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Mr. Cooper's violations of Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Personal Information; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
Breach of Express Contract
On Behalf of Plaintiff and the Class

77. Plaintiff realleges the foregoing paragraphs as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

78. Mr. Cooper provides mortgage services to Plaintiff and Class Members pursuant to the terms of its contracts, which all were a party to, including agreements regarding the handling of their confidential Personal Information in accordance with Mr. Cooper's policies, practices, and applicable law. Plaintiff not in possession of these contracts but upon information and belief these contracts are in the possession of Mr. Cooper. As consideration, Plaintiff and Class Members paid money to Mr. Cooper for its mortgage services. Accordingly, Plaintiff and Class Members paid Mr. Cooper to securely maintain and store their Personal Information. Mr. Cooper violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts.

79. Plaintiff and Class Members have been damaged by Mr. Cooper's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT IV
Breach of Implied Contract In Fact
On Behalf of Plaintiff and the Class

80. Plaintiff realleges the foregoing paragraphs as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

81. Mr. Cooper provides home mortgage services to Plaintiff and Class Members also formed an implied contract with Mr. Cooper regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for home mortgage services from Mr. Cooper and by Mr. Cooper's sale of home mortgage services, regarding the handling of their confidential Personal Information in accordance with Mr. Cooper's policies, practices, and applicable law.

82. As consideration, Plaintiff and Class Members paid money to Mr. Cooper for its home mortgage services. Accordingly, Plaintiff and Class Members paid Mr. Cooper to securely maintain and store their Personal Information. Mr. Cooper violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts or agreements.

83. Plaintiff and Class Members have been damaged by Mr. Cooper's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
Invasion of Privacy (Electronic Intrusion)
On Behalf of Plaintiff and the Class

84. Plaintiff realleges the foregoing paragraphs as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

85. Plaintiff and Class Members maintain a privacy interest in their Personal Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above. Plaintiff's and Class Members' Personal Information was contained, stored, and managed electronically in Mr. Cooper's records, computers, and databases

that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities, unique identification numbers, and financial records that were only shared with Mr. Cooper for the limited purpose of obtaining and paying for home mortgaging services. Additionally, Plaintiff's and Class Members' Personal Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Personal Information for fraud, identity theft, and other crimes without their knowledge and consent.

86. Mr. Cooper's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third parties because of its failure to adequately secure and safeguard their Personal Information is offensive to a reasonable person. Mr. Cooper's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' private quarters where their Personal Information was stored and disclosed private facts about their finances into the public domain.

87. Plaintiff and Class Members have been damaged by Mr. Cooper's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VI
Unjust Enrichment
On Behalf of Plaintiff and the Class

88. Plaintiff realleges the foregoing paragraphs as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

89. Plaintiff and Class Members conferred a benefit on Mr. Cooper by paying for data and cybersecurity procedures to protect their Personal Information that they did not receive.

90. This conferral of benefit was not incidental to Plaintiff's and Class Members'

treatment—Plaintiff and Class Members expected that Mr. Cooper would ensure that their Personal Information would remain secure and not be disclosed to unauthorized third parties by, *inter alia*, devoting appropriate and sufficient budgets to secure and protect that Personal Information.

91. Mr. Cooper has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to Mr. Cooper's conduct alleged herein, it would be unjust and inequitable under the circumstances for Mr. Cooper to be permitted to retain the benefit of its wrongful conduct.

92. Plaintiff and the Class Members are entitled to full refunds, restitution and/or damages from Mr. Cooper and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by Mr. Cooper from its wrongful conduct. If necessary, the establishment of a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation may be created.

93. Additionally, Plaintiff and the Class Members may not have an adequate remedy at law against Mr. Cooper, and accordingly plead this claim for unjust enrichment in addition to or, in the alternative to, other claims pleaded herein.

COUNT VII
Breach of Confidence
On Behalf of Plaintiff and the Class

94. Plaintiff realleges the foregoing paragraphs as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

95. At all times during Plaintiff's and Class Members' relationship with Mr. Cooper, Mr. Cooper was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Personal Information.

96. As alleged herein and above, Mr. Cooper's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

97. Plaintiff and Class Members provided their Personal Information to Mr. Cooper with the explicit and implicit understandings that Mr. Cooper would protect and not permit Personal Information to be disseminated to any unauthorized parties.

98. Plaintiff and Class Members also provided their Personal Information to Mr. Cooper with the explicit and implicit understandings that Mr. Cooper would take precautions to protect such Personal Information from unauthorized disclosure.

99. Mr. Cooper voluntarily received in confidence Plaintiff's and Class Members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

100. Due to Mr. Cooper's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiff's and Class Members' Personal Information, Plaintiff's and Class Members' Personal Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

101. As a direct and proximate cause of Mr. Cooper's actions and/or omissions, Plaintiff and Class Members have suffered damages.

102. But for Mr. Cooper's disclosure of Plaintiff's and Class Members' Personal Information in violation of the parties' understanding of confidence, their protected Personal Information would not have been compromised, stolen, viewed, accessed, and used by

unauthorized third parties. Mr. Cooper's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected Personal Information, as well as the resulting damages.

103. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Mr. Cooper's unauthorized disclosure of Plaintiff's and Class Members' Personal Information.

104. As a direct and proximate result of Mr. Cooper's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from financial fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remain in Mr. Cooper's possession and is subject to further unauthorized disclosures so long as Mr. Cooper fails to undertake appropriate and adequate measures to protect the Personal Information of patients in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

105. As a direct and proximate result of Mr. Cooper's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT VIII
Breach of Fiduciary Duty
On Behalf of Plaintiff and the Class

106. Plaintiff realleges the foregoing paragraphs as if fully set forth herein. Plaintiff

brings this claim on behalf of the Class set forth above.

107. Considering their special relationship, Mr. Cooper has become the guardian of Plaintiff's and Class Members' Personal Information. Mr. Cooper has become a fiduciary, created by its undertaking and guardianship of patient Personal Information, to act primarily for the benefit of their patients, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' Personal Information and to timely notify them in the event of a data breach.

108. Mr. Cooper has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. Mr. Cooper has breached its fiduciary duties owed to Plaintiff and Class Members by failing to:

a. properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' Personal Information;

b. timely notify and/or warn Plaintiff and Class Members of the Data Breach; and

c. otherwise failing to safeguard Plaintiff's and Class Members' Personal Information.

109. As a direct and proximate result of Mr. Cooper's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Personal Information, which remains in Mr. Cooper's possession and is subject to

further unauthorized disclosures so long as Mr. Cooper fails to undertake appropriate and adequate measures to protect patient Personal Information in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

110. As a direct and proximate result of Mr. Cooper's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on his own behalf and on behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiff as Class Representative and the undersigned as Class Counsel;

B. For equitable relief enjoining Mr. Cooper from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Personal Information;

C. For equitable relief compelling Mr. Cooper to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

D. For an order requiring Mr. Cooper to pay for credit monitoring services for Plaintiffs and the Class of a duration to be determined at trial;

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

F. Awarding declaratory and injunctive relief as permitted by law or equity to assure

that the Class has an effective remedy, including enjoining Mr. Cooper from continuing the unlawful practices as set forth above;

G. Awarding pre- and post-judgment interest to the extent allowed by the law;

H. Awarding all costs, experts' fees and attorneys' fees, expenses, and costs of prosecuting this action; and

I. Such other and further relief as the Court may deem just and proper.

DATED: November 14, 2023

Respectfully Submitted,

/s/ Joe Kendall
JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214-744-3000 / 214-744-3015 (fax)
jkendall@kendalllawgroup.com

RACHELE R. BYRD*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

JON TOSTRUD*
ANTHONY CARTER*
TOSTRUD LAW GROUP, PC
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: 310/278-2600
Facsimile: 310/278-2640
jtostrud@tostrudlaw.com
acarter@tostrudlaw.com

Attorneys for Plaintiff and the Class
**Pro Hac Vice Forthcoming*